Campus Communication
DRAKE UNIVERSITY

February 4, 1984

To: Larry Landis
From: Robert W. Lutz and George Miller
Subject: Additional Implications of Penetration

The intent of this memo is to share with you some additional thoughts on the implications for the future of computing at Drake University as a result of the recent system penetration at the behest of KWWL-TV. In this memo, we will discuss several areas of concern, all of which have impacts on service delivery to our students, faculty and staff. These impacts will be related to the University's ability to deliver our advertised curriculum to our student body. In addition to the service impacts, a set of fiscal impacts will also be presented.

BACKGROUND INFORMATION

It occurs to us that we need to define exactly for you and for the President's Staff what we mean by penetration of our academic computer system. If an individual penetrates the system, this means that the individual acquires ALL system privileges. This means that the individual may examine, modify or delete any or all programs, data or procedures stored in the system and may deny any or all other users access to any or all system resources. In other words, total control of the computer system and all stored data is placed at the whim of the intruder, and his actions are only limited by his sense of morality, which is obviously suspect.

It is also appropriate to present a brief discussion of the topic of computer security. The built-in security provisions of any computer system can be defeated by a skilled and determined "hacker". The safety of a computer system is a blend of the security provisions of the system itself and the perception of the "hacker" as to the determination of the owner of the computer system to exact retribution for security violations. Over the past four years, the fact that Drake University has not experienced a single system penetration may be attributed to our well-known, swift response to questionable practices by members of our user community. Thus, with limited funds and a small staff, we have been able to provide a high level of security to users with a computer system which is noted for providing a high-quality, user-friendly service with a minimum of system-imposed restrictions on the users. The ability of KWWL-TV to influence individuals of dubious moral character to penetrate our system, may well have been based on their presentation to the "hackers" of Drake University as a NEW TARGET, rich with the promise of challenging security

arrangements, interesting data files, unusual programs, etc. They may well have initiated a cycle of testing to attack our system which might not otherwise have occurred without the legitimitizing influence of a large news-gathering organization.

IMPLICATIONS OF IGNORING THE PENETRATION

Now, let us consider the situation in which we in the Computer Center make no changes in our daily routine as a result of the penetration. In other words, we ingore the fact that this penetration occurred. We recognize the fact that knowledge of the penetration's occurrence will continue to spread throughout the Drake and wider communities. In particular, since there is strong evidence that the "hackers" involved were students or ex-students at Iowa State, and since we have been told by Iowa State personnel that the rumor mill regarding the penetration indicates that as many as six Iowa State students were involved, we must presume that we will now become a target of these "hackers" in the future.

Let us consider what may occur under these circumstances, and consider the impacts on our students, our faculty and staff, and on the external community. We draw on the experiences of the Computation Center at Iowa State University, which operates four VAX systems for instructional computing for Iowa State students. These systems are routinely penetrated by "hackers". Examples of their actions include deletion and modification of the operating system which at times denies all users access to particular functions and capabilities; deletion of all files owned by an instructor relating to a particular course which resulted in major inconvenience to the instructor and to all students in that course; gaining access to the passwords of other students and use of those students accounts (which are limited to a prescribed amount of computing during the semester) which then denies computer availability to the effected student. The problems which have been illustrated represent major concerns of those Computation Center staff members who are charged with maintaining a computing environment which is beneficial to all the ISU student body.

Since the VAX systems at Iowa State are used only for instructional computing, the major impacts fall directly on the student users of the system, and those faculty users who are using the system for instruction in their classes. The impacts on the Drake student body will be magnified since we have a single VAX to support our student users, while Iowa State operates four VAX systems. Once our system is penetrated, we have no alternate system which can be used to provide service. We must again reiterate that these problems at Iowa State continue since no substantive action has been taken against any student "hacker" who has been identified as having caused trouble. The "hackers" operate with the

knowledge that they will not be held accountable for their actions.

Following discovery of the recent penetration of the Drake system, it was necessary to remove the VAX from service to perform a minimal damage assessment. This service disruption lasted for seven hours and caused our student body great anxiety regarding their ability to complete assignments, and concern that materials which they had entered into the computer may have been lost forever. Further penetrations will make this type of service disruption a commonplace event. Obviously, the ability of Drake University to deliver our advertised curriculum to our students will be severely jeoprodized. Student and faculty reactions to previous service disruptions and lack of ability to deliver required service levels are well known to us all.

The impacts of "hacking" will effect Drake students and faculty in additional ways that do not occur at Iowa State. For example, our VAX is used to provide a test-generation and test-scoring system. The service uses large data banks of test questions and answers which are stored on disk. Since an intruder can access any data file on the system, the confidentiality of these question and answer banks must be considered compromised, and the enormous amount of labor expended by both faculty and Computer Center staff in the construction of these data banks rendered useless. In addition, it is also possible for the intruders to modify the question and answer banks, WITHOUT DETECTION, and to randomly change answers. Obviously, the result of this action would be to destroy the validity of the material.

The use of the computer to prepare examinations has been of great benefit to many faculty members, who operate with limited clerical support. The added workload of returning to manual methods of test preparation, detracts from time which the faculty can spend with their other duties such as class preparation, student counseling, research and service activities. In addition, the test generation system enables faculty to develop higher quality questions by performing otherwise time-consuming item analyses on the tests taken by students. Clearly, loss of this service would adversely effect our student body.

Our faculty will also be effected in other ways. Since all faculty research computing makes use of the VAX, we must also consider the impact of penetrations on this type of usage. A portion of our faculty research is done under contract with various businesses and governmental organizations. These contractors insist upon maintenance of confidentially in the treatment of all data and analyses and reports of the results. If we cannot maintain this level of security, we cannot provide computer support for this type of research.

Let us next consider the impacts of penetration on administrative users of the VAX. Recently, we have been very busy using the PLANTRAN system for budget projections. The total set of University budget data would be available to the penetrators. We are sure that our trustees would not approve of the intruder's examination of our confidential planning data. Let us hope that KWWL-TV did not discover these files during the penetration this week. Our trustees would also not likely appreciate being presented the budget on TV or in the newspaper under the guise of First Amendment rights and/or freedom of information.

Other sensitive information stored on the VAX includes data which has been moved from the administrative system for institutional research projects. For example, a categorization of admissions applicants based on high school rank and standard test score was recently completed for the Vice-President for Student Life. Data on individual students must be safeguarded under Buckley amendment considerations. Sensitive data has also been stored by Bill Klipec during the course of his research on student mobility within the University. These materials include performance data, progress toward a degree information, etc.

A number of administrative offices use the VAX for word-processing. The Vice President for Academic Administration prepared last fall's Academic Division report to the Board of Trustees using the VAX. Our trustees again would not likely appreciate being presented their semi-annual report on TV or in the newspaper under the guise of First Amendment rights and freedom of information.

Both Cowles Library and the Law Library provide students with up-to-date information regarding library serials availability using programs on the VAX. These computerized systems must be accurate to be useful to students and faculty. An intruder could easily modify or delete these large data systems thus rendering them useless to the Drake community and destroying thousands of hours of work.

The complete nutritional program offered to our students by Hubbell Dining Hall is based upon a computerized system operating on the VAX. This system consists of programs which maintain inventories, calculate the nutritive value of meals, and aid in the preparation of menus which provide all required nutritive components on a daily, weekly and monthly basis. Deletion or modification of this system would wreak havoc on this vital service to our students.

The Athletic Department uses the VAX for a number of tasks. For the Drake Relays the VAX is used to qualify competitors, to report results, and to maintain ticketing information. The system is also used to maintain Bulldog Club records, mailing lists, etc. Finally, an extensive computerized analysis system is operated for the staff of the

football program.

Next let us consider the impacts on external users served by the Drake University Computer Center. Two of our major external users are Meredith Corporation and the Des Moines Register and Tribune. Both of these organizations use the VAX to do market research studies and to analyze various surveys. The information which they manipulate is obviously confidential to these organizations. We must expect that they may reconsider their use of our computer system in view of the recent penetration. Loss of these two users would have two effects. The first is the loss of income required to maintain Computer Center services to students, faculty and staff. The second is the loss of a valuable service to the Des Moines community with attendant impact on the reputation of Drake University. Of course, these two organizations are not our only external users. Other external users include Des Moines Water Works, American Federal Savings, First Iowa State Bank, United Federal Savings, Kirke-Van Orsdel, Shearson/American Express, Pioneer Hi-Bred International and others.

As a result of the recent penetration, we now must be concerned with our capability to abide by licensing agreements for various proprietary software products. Under terms of these licenses, we must protect the rights of the copyright holders or be subject to potential liability for damages. Such licenses exist for SPSS (Statistical Package for the Social Sciences), BMDP (BioMedical Computer Programs), COMPUSTAT (a data base service from Standard and Poor), and PLOT10 (graphics software from Tektronix). You may recall the involvement of Jim Cooney a few years ago when an old version of SPSS was stolen from Drake University and appeared on the computer of a service bureau in Omaha.

IMPLICATIONS OF TAKING ACTIONS FOR PROTECTION

Let us now consider actions which might be taken by Drake University in response to the penetration which has been accomplished. These actions may be separated into two categories, actions which will aid in the detection of a penetration, and actions which will reduce the likelihood of penetration or will limit damage following a penetration.

Detection of system penetrations and identification of the perpetrators will be signficantly enhanced if we initiate a process called Image Accounting. This process consists of forcing the computer system to record not only information about computing resources used, such as central processor time, pages printed, etc., but also to record the name of every program run by every user on the system. These enhanced accounting records must then be scanned by programs written by Computer Center staff for purposes of identifying illegal actions and processes. The value of this action will be not only to identify the perpetrators, but to provide

direct indication of the techniques used to accomplish the penetration. Corrective actions can then be taken to prevent further penetrations using the same technique.

Use of Image Accounting for these purposes will require increased use of computer and personnel resources. The increased disk storage requirements to operate Image Accounting will add significantly to the pressing demands for this critically short resource. We will have to modify our proposals for disk storage expansion, which are under development, to provide for the additional space. Examination of the image accounting records on a routine basis will require large amounts of computer time and would seriously impact our student user community if we were to perform this analysis prior to midnight on any day. Thus, it will be necessary to perform this analysis after midnight; causing serious deterioration of service offerings to our faculty researchers who are restricted to overnight service since their priorities are lower than those of the students.

There are two possible action options which may be taken to reduce the likelihood that a penetration will occur. The first option is to remove several commands from the system which are suspected to offer possibility of misuse. These commands have been installed by DEC over the years to make it easier for responsible users to effectively and efficiently utilize system resources in a user-friendly manner. Removal of these commands will have an adverse effect on all users by forcing them to go through more complicated command structures to accomplish their tasks.

The second option will be to remove all dial-up ports from the system. This option will deny access to all students who have their own microcomputers or terminals and who are presently accessing the system from residence halls, fraternities and sororities, and from apartments or their homes. We will also deny access to faculty and staff users who rely on such access methods in the course of their daily routines. This option will force all users to terminals which are hard-wired on our own buried campus cable system. We then need only control access to our campus terminals to screen out potential intruders. To make this option complete, we must then require presentation of identification by all users to appropriate security officials at the location of all terminals. There are again two costs involved with the option. The first is in inconvenience to users; the second is the cost to modify our identification systems to insure no intruder can gain access to a campus terminal.

There are two possible action options which can be taken to minimize the risk due to a penetration. The first involves rewriting the facility which is used to authorize use of the computer. The goal of this project would be to incorporate a password system to erect another barrier which

will help prevent use of the authorization program even after a system penetration has occurred. The second option is to modify the manner of processing of sensitive information by prohibiting the storage of such information on a disk. That is, all sensitive data must be stored only on tape, so that operator intervention is required to access the data. Some current projects cannot be dealt with in this manner. For example, the current PLANTRAN system can be treated either by reverting to a totally card-oriented environment, or by moving the system to the Honeywell computer. Reverting to cards will at least triple the personnel time involved in preparing data for these modeling activities. Moving the system to the Honeywell computer will required an expenditure of $395 per month to add a FORTRAN compiler to the Honeywell system. In addition, since that system only runs at about one-fourth the speed of the VAX, it can be expected that current complete runs which now take about seven hours on the VAX and use about a half-hour of central processor time, will require more than twenty-four hours to complete. Obviously, these techniques will have serious impacts on the various user communities, students, faculty, administrators and external users.

More careful study may reveal additional alternatives which can be considered. All options outlined above will of necessity require significant Computer Center staff time for their development and implementation. It is clear, therefore, that the user community will be denied their normal ready access to an already hard-pressed staff.